L10 - Effective Design Methods for Integrating Safety Using Logix Controllers

For Classroom Use Only!

LISTEN. THINK. SOLVE.®

Allen-Bradley • Rockwell Software

Rockwell Automation

Important User Information

This documentation, whether, illustrative, printed, “online” or electronic (hereinafter “Documentation”) is intended for use only as a learning aid when using Rockwell Automation approved demonstration hardware, software and firmware. The Documentation should only be used as a learning tool by qualified professionals.

The variety of uses for the hardware, software and firmware (hereinafter “Products”) described in this Documentation, mandates that those responsible for the application and use of those Products must satisfy themselves that all necessary steps have been taken to ensure that each application and actual use meets all performance and safety requirements, including any applicable laws, regulations, codes and standards in addition to any applicable technical documents.

In no event will Rockwell Automation, Inc., or any of its affiliate or subsidiary companies (hereinafter “Rockwell Automation”) be responsible or liable for any indirect or consequential damages resulting from the use or application of the Products described in this Documentation. Rockwell Automation does not assume responsibility or liability for damages of any kind based on the alleged use of, or reliance on, this Documentation.

No patent liability is assumed by Rockwell Automation with respect to use of information, circuits, equipment, or software described in the Documentation.

Except as specifically agreed in writing as part of a maintenance or support contract, equipment users are responsible for:

- properly using, calibrating, operating, monitoring and maintaining all Products consistent with all Rockwell Automation or third-party provided instructions, warnings, recommendations and documentation;
- ensuring that only properly trained personnel use, operate and maintain the Products at all times;
- staying informed of all Product updates and alerts and implementing all updates and fixes; and • all other factors affecting the Products that are outside of the direct control of Rockwell Automation.

Reproduction of the contents of the Documentation, in whole or in part, without written permission of Rockwell Automation is prohibited.

Throughout this manual we use the following notes to make you aware of safety considerations:

WARNING

Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.

IMPORTANT

Identifies information that is critical for successful application and understanding of the product.

ATTENTION

Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you:

- identify a hazard
- avoid a hazard
- recognize the consequence

SHOCK HAZARD

Labels may be located on or inside the drive to alert people that dangerous voltage may be present.

BURN HAZARD

Labels may be located on or inside the drive to alert people that surfaces may be dangerous temperatures.

Effective Design Methods for Integrating Safety Using Logix Controllers

Contents

Before you begin 5

About this lab 5

Tools & prerequisites 5

Getting Started 6

Safety Task 7
Safety Tags 10
Mapping Tool 12
Safety Input Instructions 13
Safety Output Instructions 18
Diagnostics 20
Discrepancy Faults 23
Channel Cycled Input Fault 25
Pulse Test Fault 25
Safety Signature 28
Safety Lock 30

Before you begin

This lab assumes a basic understanding of RSLogix 5000 software.

About this lab

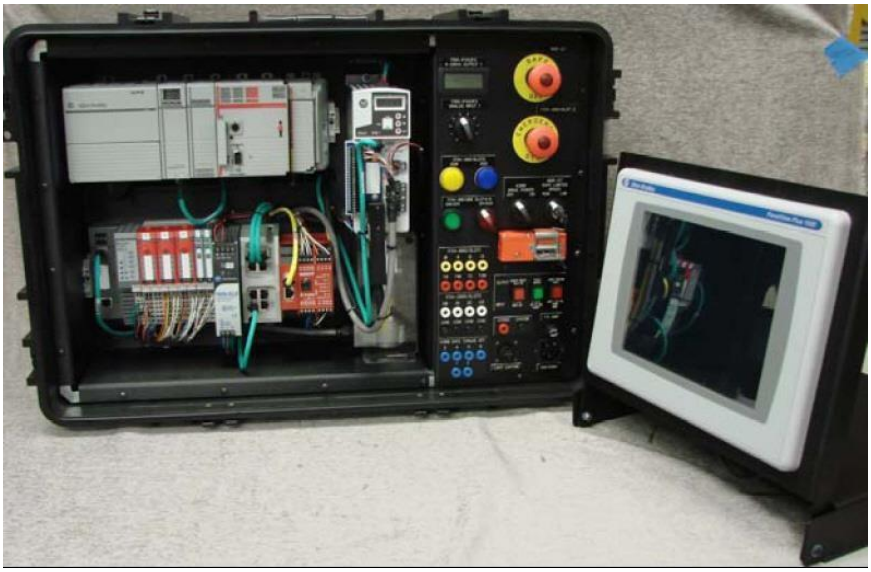
In this lab, you will see how Rockwell Automation has integrated safety products, features and functions into an environment that allows effective and efficient programming for your safety needs. Parallel safety processing, dedicated safety tasks in the PLC, certified safety function blocks and safety I/O handling work together allowing you to achieve your safety goals in a much simpler, straightforward manner.

This lab takes approximately 90 minutes to complete.

Tools & prerequisites

The following software programs, hardware, and files are required for use with this lab.

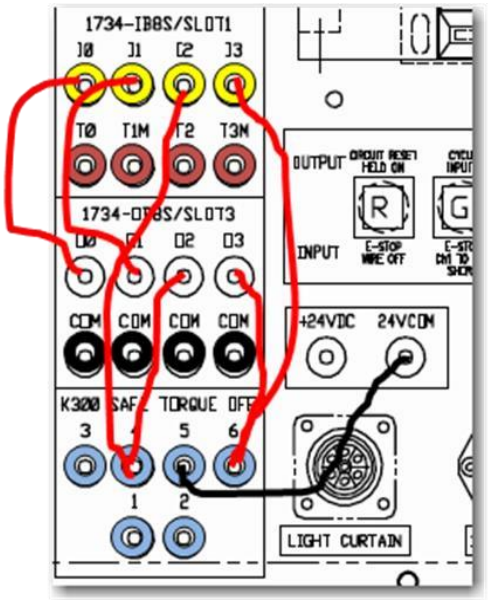
- Software Programs:
- RSLinx Classic 2.59 or later
- RSLogix 5000 Professional v20 or later ▪ Hardware Devices:
- Compact Machine Solutions Demo Case ▪ Files required:
- Compact GuardLogix – GuardLogix_StartingPoint
- Compact GuardLogix – GuardLogix_DCA_SafetyLockDemo
- PanelView Plus 1000 - CMSS_Demo_DCAfaceplate.mer
- MSR57 - CMSS_Core_Demo.csf



Getting Started

The '**GuardLogix_StartingPoint.ACD'** file should already be loaded. Please verify that the program is running and the case is ready for the lab by performing the following:

1. Verify the seven jumper cables are attached as shown:



I0 to O0
I1 to O1
I2 to 4
I3 to 6
O2 to 4
O3 to 6
5 to 24VCOM

2. Set the potentiometer to 5 on the dial.

   The potentiometer controls the speed of the motor. The value of 5 is well below the safe speed threshold configured in the MSR57P.

3. Verify the MSR57P safe limited speed key switch is set to the **RUN** position.

4. Verify the K300 Drive Power key switch is in the **ON** position.

5. If the Safe Off pushbutton is flashing, release it.

6. If the Emergency Stop pushbutton is flashing, release it.

7. The red selector switch (**Fault Reset**) is flashing, cycle it from the counter-clockwise left position to the clockwise right position and back to the left.

8. The green button (**Safety Circuit Reset**) is flashing; press it to energize the K300 safety enables.

   The 'K300 Status' light should energize. The light indicates the K300 Safety inputs are energized. You should hear the drive/motor energize, but the motor is not turning.

9. The yellow button (**Start Drive Motion**) is flashing; press it to start drive motion.

Safety Task

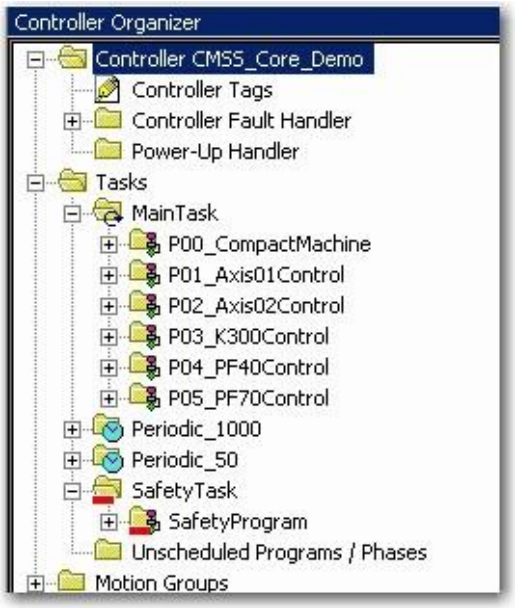
Compact GuardLogix is a CompactLogix with integrated safety, certified to be used in safety control systems up to SIL3 (IEC61508), CAT4 (EN954-1) and PLe (ISO13849-1). It performs all of the same functions as a standard CompactLogix in addition to performing safety control. To achieve these safety ratings GuardLogix uses a 1oo2 dual controller architecture. The two controllers are called the primary (left slot) and the partner (right slot).

- The primary controller runs both the standard and safety tasks
- The partner controller runs only the safety task

The primary and partner controllers compare the outputs generated by the safety task. If they ever disagree, GuardLogix will go to the safe state (de-energized).

Compact GuardLogix is configured with a single software package, RSLogix 5000, simplifying your engineering efforts. You create a single project to manage both your standard and safety code.

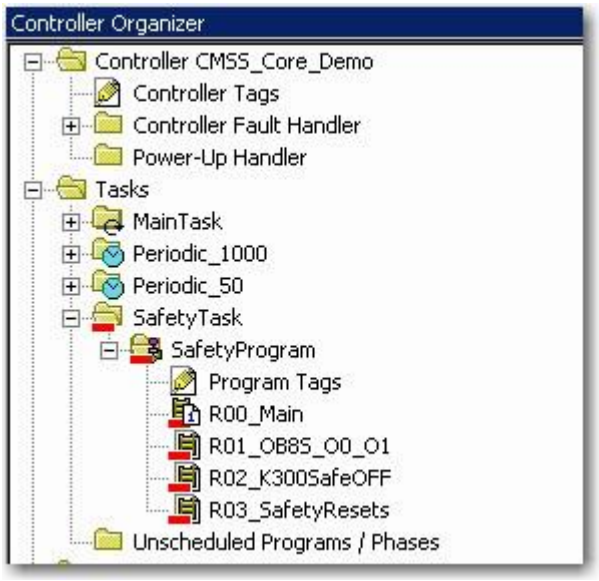
1. Open the **GuardLogix_StartingPoint.acd** file on the desktop.



A single project contains both the standard and safety code.

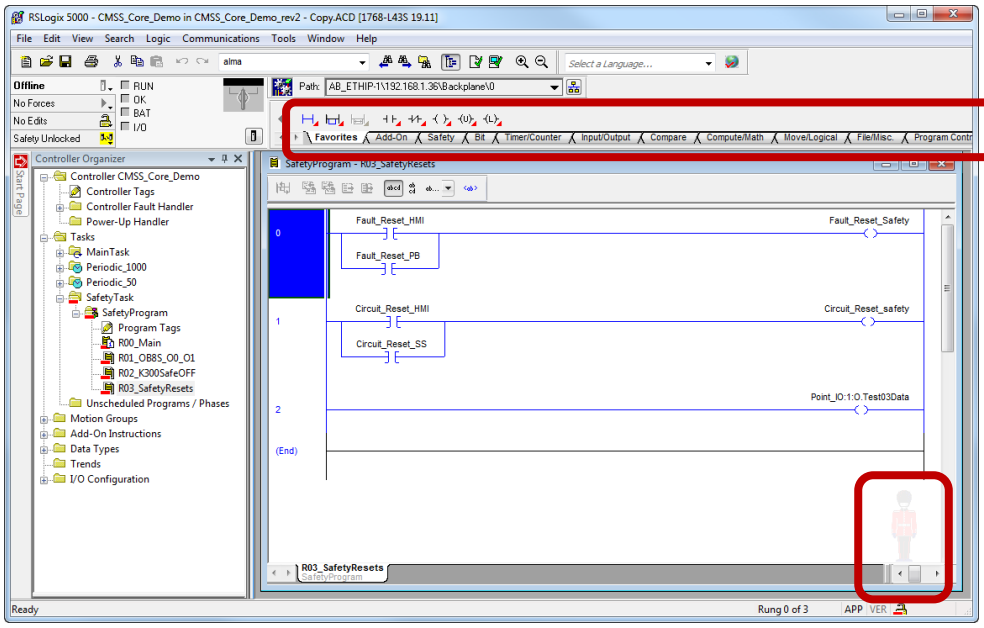
2. Go online with the controller

3. Expand the **SafetyProgram** in the **SafetyTask**



All of the safety code is contained within the Safety Task. It has the same structure as a standard task; but it is unique in that it is scanned in both the primary and partner processors. The red bar under the routines and folders in the safety task indicate these routines perform safety logic.

4. Double-click **R03_SafetyResets** routine in the **SafetyProgram** to open the routine.



If the ladder code looks typical, it should. The only unique feature of code within the safety task is that it is scanned twice, by both the primary and partner controllers.

Notice the Guard safety icon in the bottom-right side of the MainRoutine window, indicating you are accessing safety code. Also notice the red labels on the instructions available in the safety task. These instructions are certified for use in the safety task. Select some of the other instruction tabs to see what instructions are available within the safety task.

5. Close the **R03_SafetyResets** routine

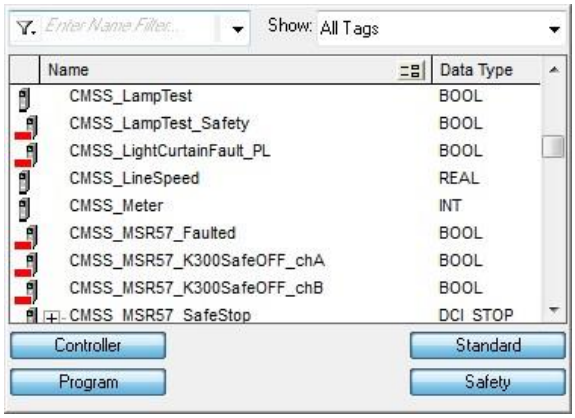
Safety Tags

A special class of tag called a Safety tag is used within the Safety Task. The integrity of a safety tag is protected because they can only be written to by logic within the Safety Task. However, Safety tags can be read in the Standard or Safety Task.

1. Open the **R00_Main** standard routine in the **P00_CompactMachine** program in the continuous task and scroll to the end of the program.
2. Add a rung, enter an XIC instruction, and select the drop down list.

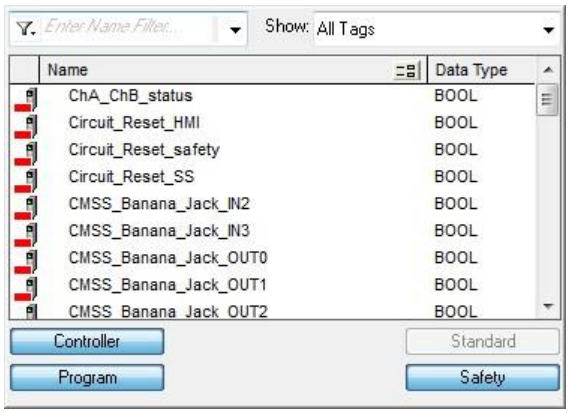
   As you scroll through the tag list, what kind of tags are available to select? You should be able to select either a standard or safety tag

   Safety tags have a red bar on the icon to the left of the tag. Standard tags do not.



3. Cancel the pending rung edits
4. Open the **R00_Main** safety routine in the safety task.
5. Add a rung at the end of the program, enter an XIC instruction, and select the drop down tag list.

   As you scroll through the tag list, what kind of tags are available to select? You should be able to select only safety tags.



6. Cancel the pending rung edits

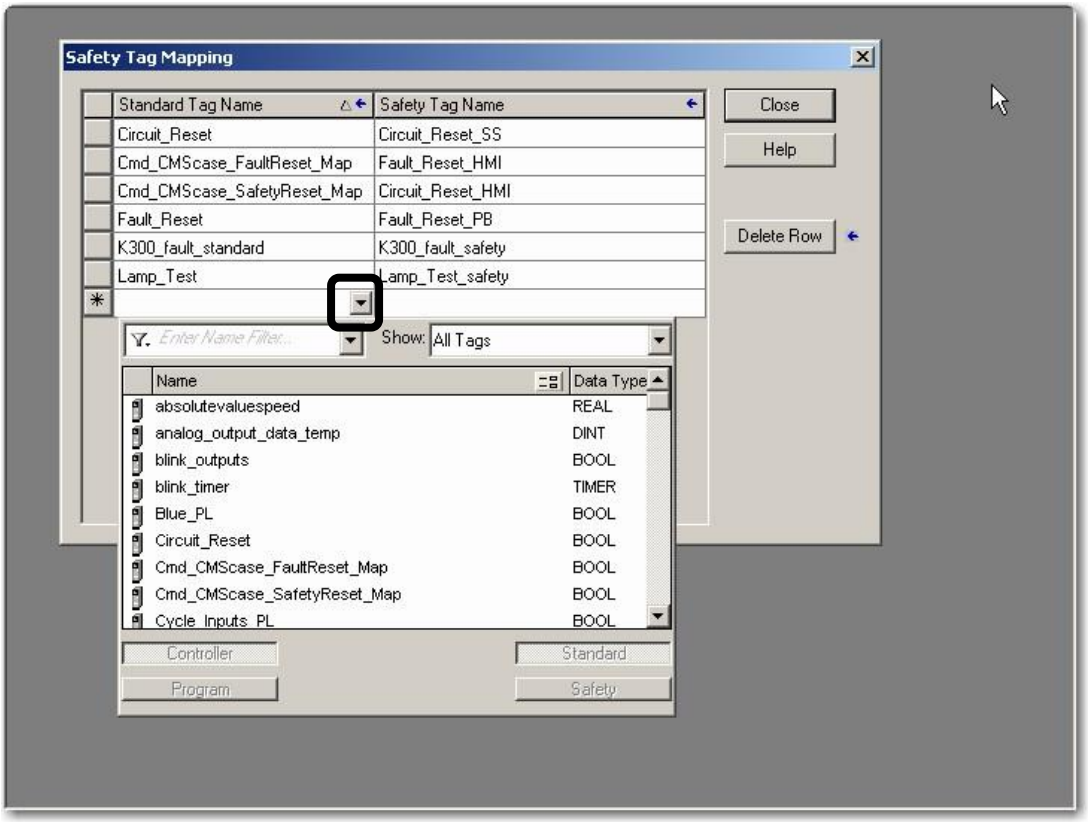
Prior to safety PLCs users would hardwire the auxiliary contacts on all of their safety devices back to the standard PLC for status information. This practice is obsolete with the GuardLogix because this status information is readily available for the standard side of the application with the Safety Tags.

7. Close any open routines

Mapping Tool

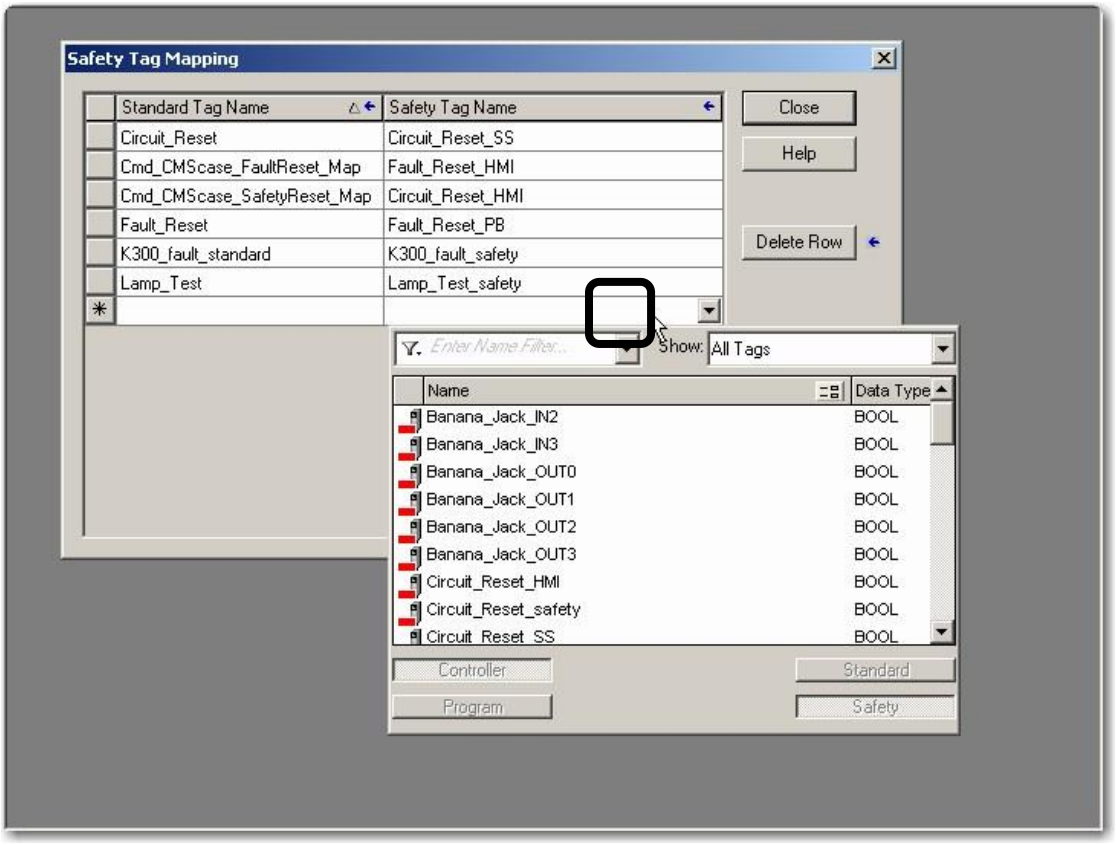
1. Select the *Logic* pulldown and *Map Safety Tags*

2. Click on the pulldown for a new standard tag (circled below)



Note that only standard tags are available

3. Click on the pulldown for a new safety tag (circled below)



Note that only safety tags are available.

This tool directly maps a standard tag to a safety tag. That safety tag can now be used in the safety task. Note that this safety tag must still be considered a standard tag in terms of safety.

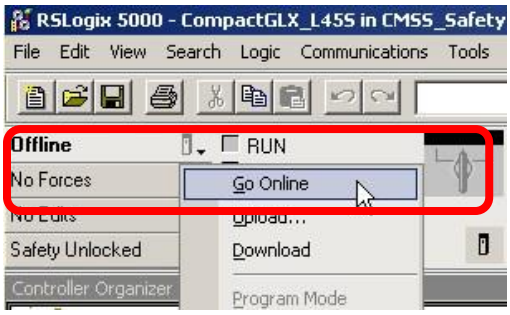
4. Close the Safety Tag Mapping window using [Close]

Safety Input Instructions

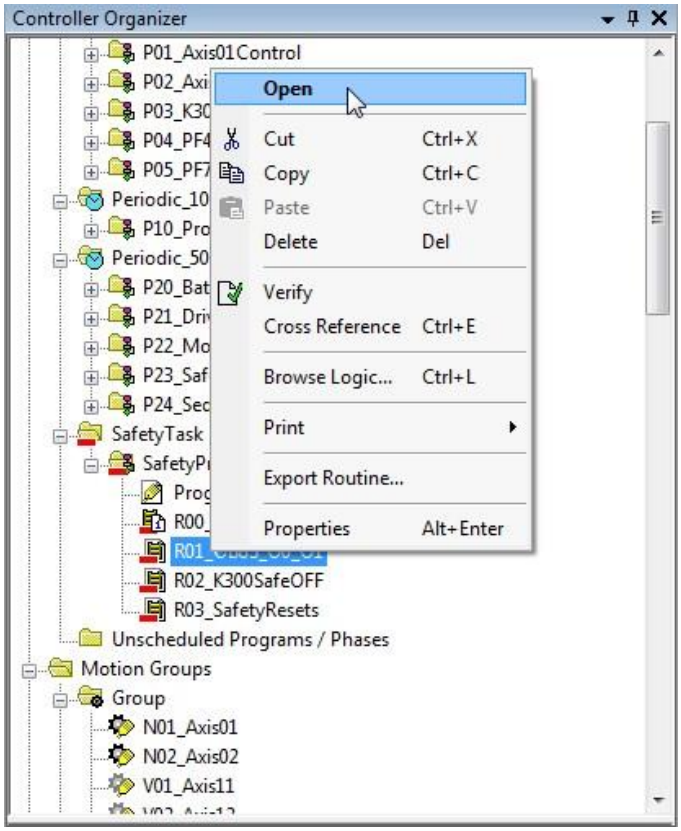
The safety input instructions are located in the 'safety' instruction tab. These instructions all have one thing in common. They assume that the input device has two channels.

1. If it is not already open, open the **GuardLogix_StartingPoint.acd** file

2. If not already, Go online with the controller:

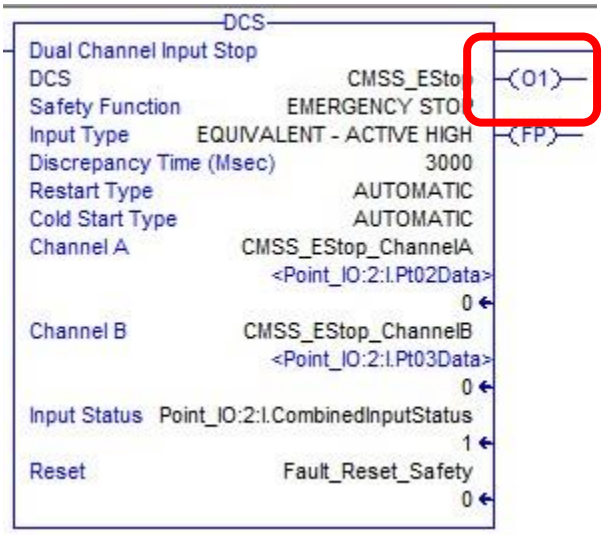


3. Call up the safety routine named **R01_OB8S_O0_O1:**



In rung 0 there is a DCS safety instruction. DCS stands for Dual Channel Stop. This instruction monitors the Emergency Stop button labeled Emergency Stop (bottom estop button).

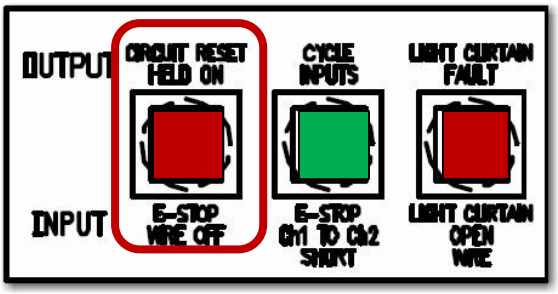
4. Press the Emergency Stop button (bottom E-Stop button) and note that the DCS output in rung 0 goes LO:



5. Release the lower Emergency Stop button on the demo case.

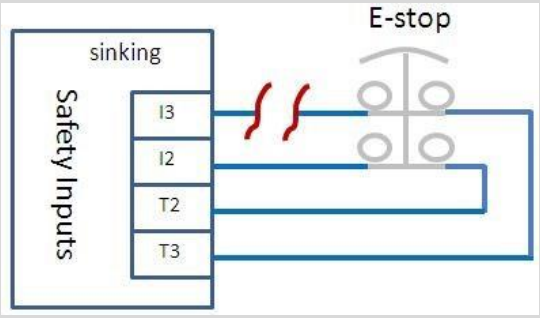
   When you cycle the Emergency Stop button on the demo case, notice that the output O1 simply follows the state of the button. This is caused by the AUTOMATIC restart parameter for Restart Type. Automatic means a manual reset is not required to energize the DCS output O1 after a 'normal' restart. Normal means that there are no faults and this is not the initial power-up.

6. To simulate a discrepancy fault, press **the E-STOP WIRE OFF** button on the demo case. It is a maintained button. Verify that it remains de-pressed.

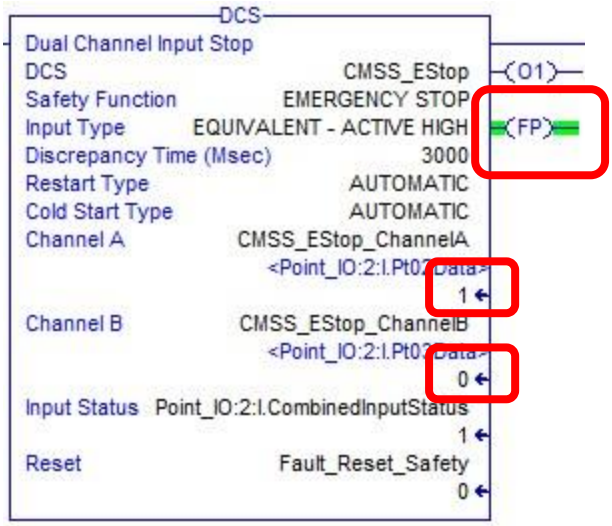


What does pressing this button do?

It causes Channel B of the Emergency Stop button to drop out (input 3 on the IB8S in slot 2):



The channels are now in different states, and if they remain in different states until the 3 second discrepancy timer expires, the DCS declares a fault. Note the FP (Fault Present) output is HI.



7. Fix the fault by pressing the **E-STOP Wire OFF** button again to return it to its normal state.

Input 03 on the 1734-IB8S in slot 2 should be HI.

8. Cycle the flashing red selector switch to reset the fault on the DCS instruction.
9. Cycle the Emergency Stop button (flashing) to prove that the fault that caused the discrepancy has been repaired.

   Note that this energizes the output O1 of the DCS
10. Press the flashing green safety reset button to energize the STO outputs; enabling the drive to operate.
11. Press the flashing yellow motion start button.

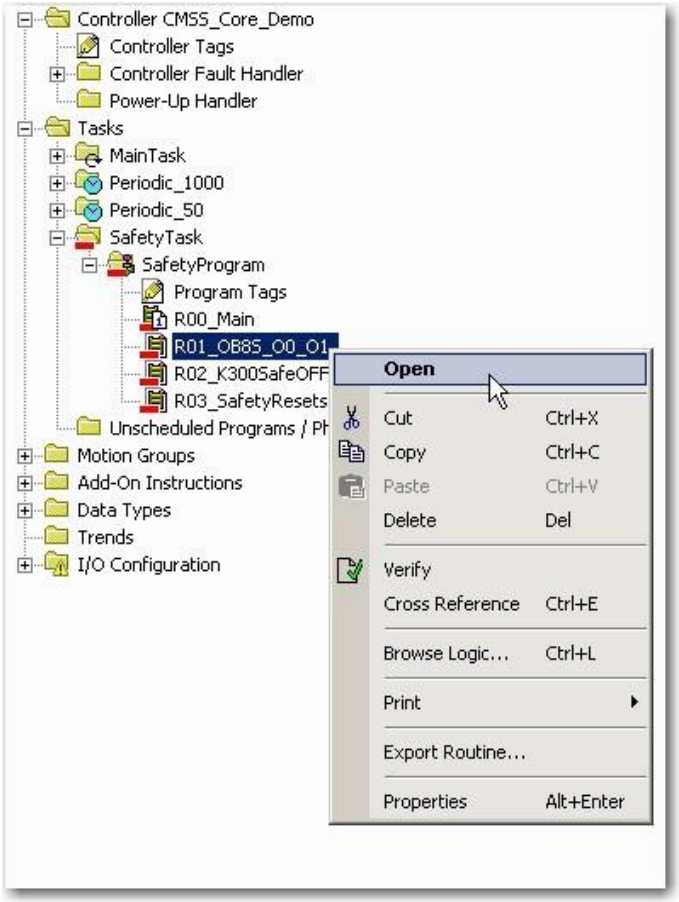
To summarize, the DCS instruction monitors dual channel devices and sets the output when both channels are in the active state (HI), and proper restart actions are completed. If the channels are not equivalent for longer than the discrepancy time, a fault is declared.

Many of the other safety input instructions simply build onto this base functionality.

Safety Output Instructions

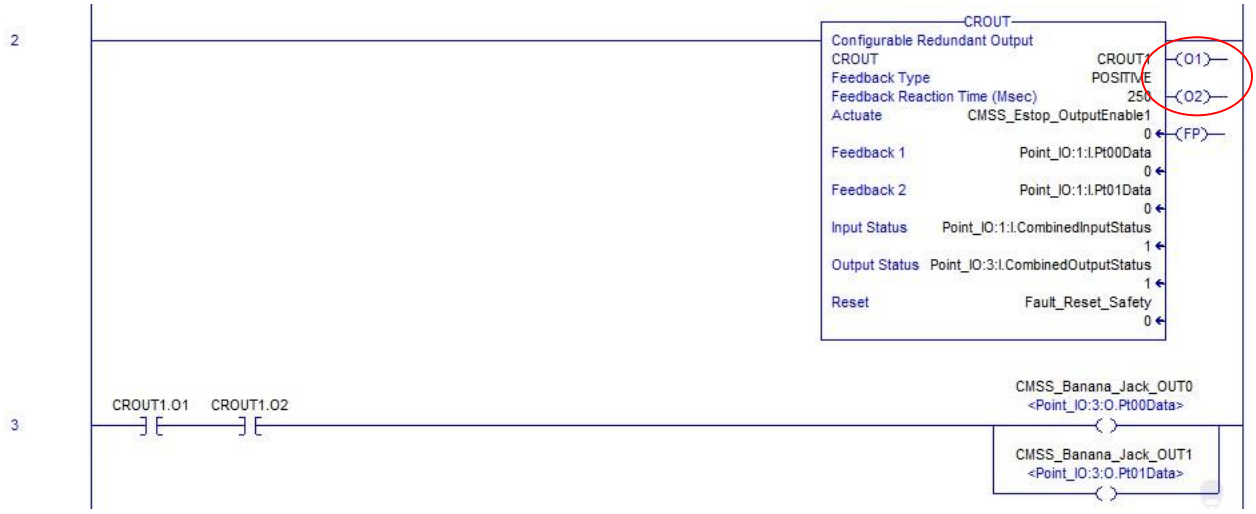
There actually is only one (1) safety output instruction, **CROUT.** The CROUT instruction controls two (2) outputs and monitors feedback. When the outputs change state, the feedback is expected to follow within a configurable reaction time. Essentially, the
CROUT has similar functionality as a safety relay.

1. If not already open, open the **R01_OB8S_O0_O1** safety routine:



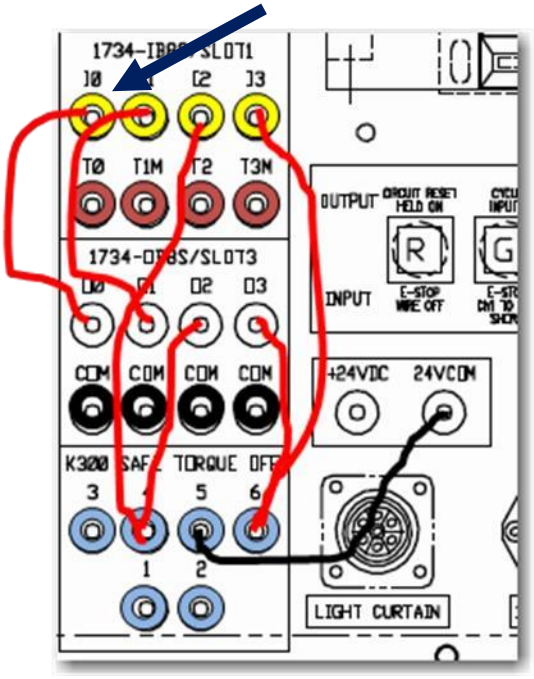
2. Scroll to rung 2 where the CROUT instruction is located.

3. If necessary, Press the flashing green fault reset button to energize the CROUT outputs. (circled below)



This CROUT instruction is being used to drive Safety Outputs O0 and O1 on the white banana jacks. We have already connected cables from those outputs to safety inputs I0 and I1 on the yellow banana jacks. These are the feedback signals for the CROUT. Since the instruction is configured for POSITIVE feedback, the feedback should be LO when the outputs are LO and HI when the outputs are HI.

4. Pull off the banana jack cable going to I0 on the 1734-IB8S module to simulate a feedback fault.



If either of the feedback signals unexpectedly drops out, the CROUT will fault.

If you wish to see the fault code associated with this fault, monitor the CROUT1.FaultCode tag. Change the Radix to Hex and you will see the fault code is 5001h. Look at the help associated with this instruction to see what this fault code refers to:

5001H	Feedback 1 turned OFF (0) unexpectedly	Check the feedback 1 signal. Reset the fault.

Why did Feedback 2 also go LO? Because when the instruction faulted, the outputs were dropped out. This causes both feedback channels to drop out as well.

5. Re-attach the banana jack cable to I0.
6. Cycle the flashing red fault reset to clear the fault.
7. Press the flashing green circuit reset button to turn the CROUT outputs back on.
8. Press the flashing yellow button to start drive motion.
9. Close the **R01_OB8S_O0_O1** safety routine and controller tag window (if open).

In summary, the CROUT instruction controls dual outputs and monitors up to two (2) feedback channels.

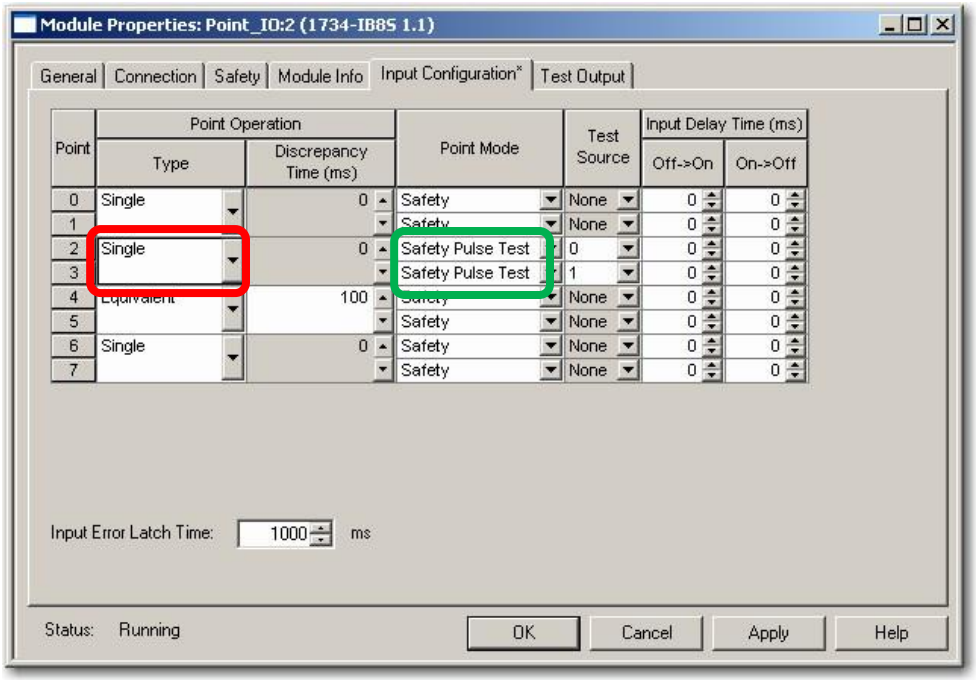
Diagnostics

From a safety perspective, it is critical that a safety device operate properly when a demand is placed on it. This is typically accomplished using redundancy and diagnostics. Redundant channels allow you to tolerate a single fault, and diagnostics allow you to detect that fault and keep your machine from restarting with that fault.

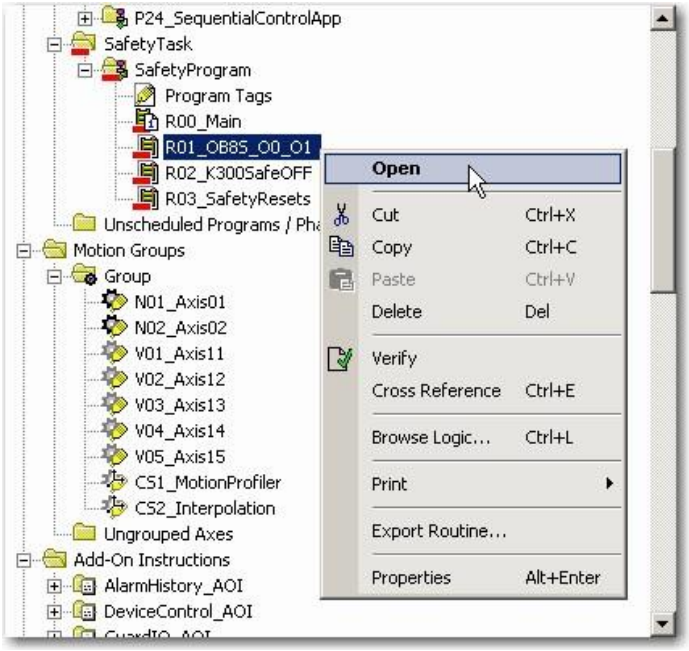
By wiring each individual safety device to a separate channel in the traditional PLC fashion, you can provide granular diagnostics for your operators and maintenance personnel. If the machine stops, HMIs can instantly direct maintenance personnel to the proper device, reducing MTTR (Mean Time to Repair).

The Emergency Stop is wired to channels 2 and 3 on the 1734-IB8S PointGuard input module. The configuration of this module is shown below. Channels 2 and 3 are configured for Single Point Operation as well as pulse testing.

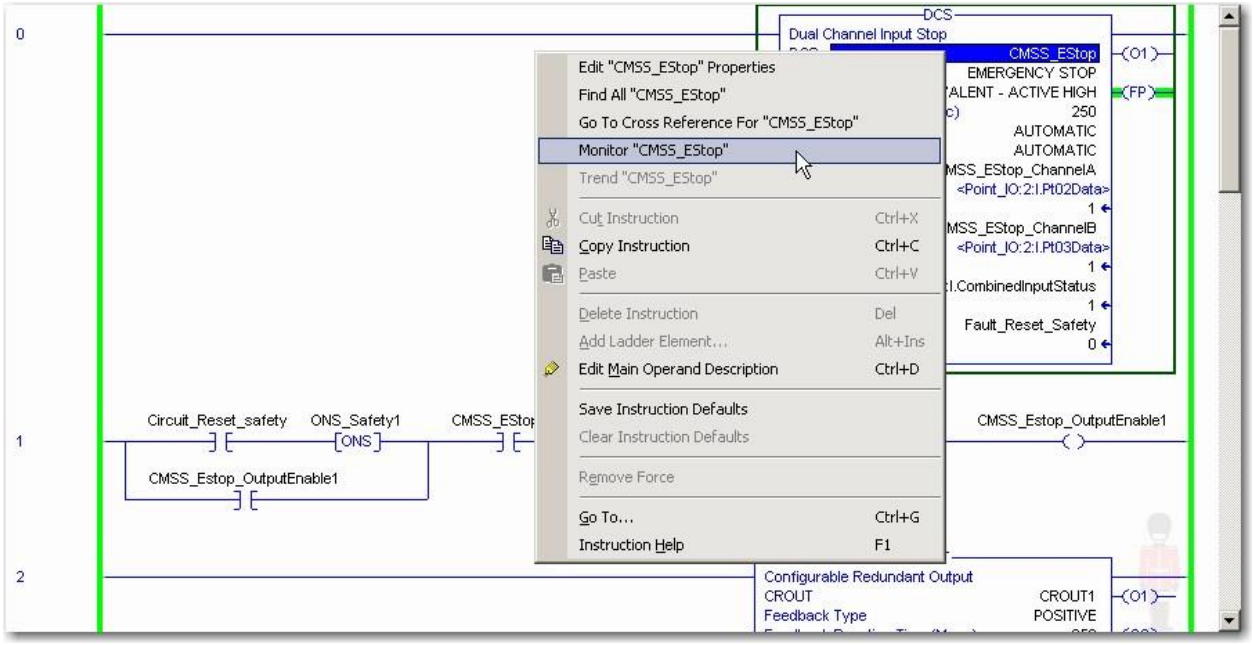
If configured for single channel, discrepancy faults can be detected by the dual channel safety instructions, providing instruction defined tags that make it easy to diagnose and annunciate fault(s) on your HMI.



1. If not already open, right-click **R01_OB8S_O0_O1** in the safety task and select **Open**.

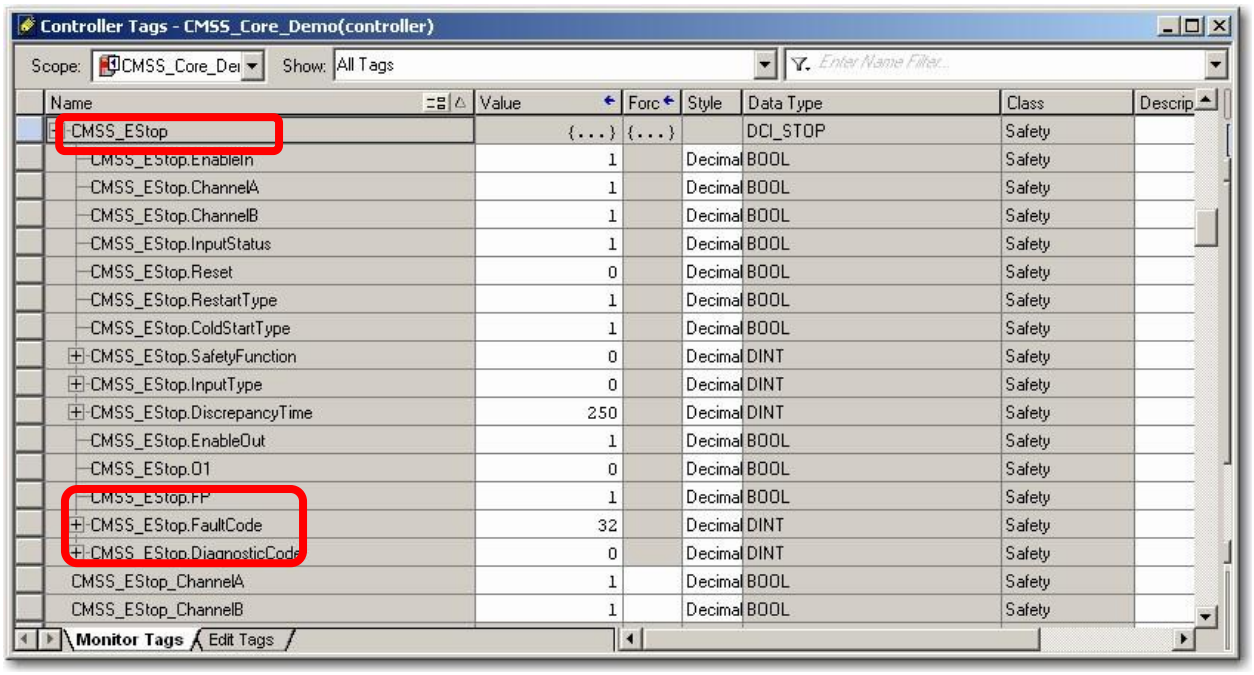


2. Right click on the tag **CMSS_EStop** in the DCS instruction on rung 0, and Select **Monitor CMSS_EStop**



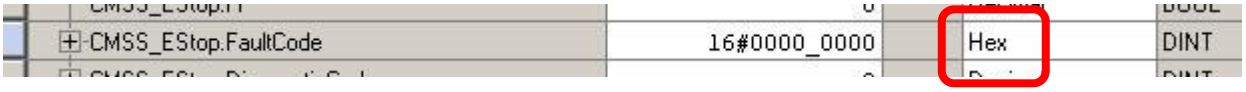
The instruction used to monitor the Emergency Stop button is a DCS, Dual Channel Stop.

3. Expand tag **CMSS_EStop** (this is the first tag in the list):



These instructions have predefined tags that include fault codes.

4. Locate the tag called ***CMSS_EStop.FaultCode*** and change the style to HEX. Click on the window circled below and select Hex from the pulldown.



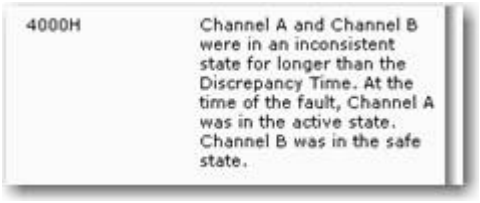
The fault codes in the user's manual and instruction help are shown in Hex.

5. If necessary, press the flashing green reset button to reset the fault code to 0.

Discrepancy Faults

6. Press the 'EStop wire OFF' button to generate a **discrepancy fault**

When the E-Stop wire off button is pressed, the normally dual equivalent channels go to diverse states; one HI and one LO. The safety system stops the motor because one of the E-Stop channels went LO. Note that this is the same condition that would occur if there was a short around one of the contacts when a demand is placed on the device. The discrepancy fault code 4000h indicates precisely that channel A was HI while channel B was LO, which is correct since the wire OFF affects channel B.


4000H
Channel A and Channel B were in an inconsistent state for longer than the Discrepancy Time. At the time of the fault, Channel A was in the active state. Channel B was in the safe state.

7. Press the Flashing red EStop DCS icon on the HMI:

8. Press the Fault button on the bottom of the HMI screen:

The DCS instruction faceplate for the Emergency Stop button provides the same information to the operator. It provides the exact description of the 4000h code as found in the user's manual.

9. Close the instruction faceplate on the HMI using the [X] in the top right corner.

10. Press EStop wire OFF button again to fix the fault.

When the wire off is fixed, the channels both return to HI and are equivalent. But the safety system will not allow the motor to restart because it assumes one of the contacts still has a short around it.

11. Cycle flashing red fault reset switch to clear the fault code.

12. Cycle the Emergency Stop button (flashing).

You must prove that the short around the contact has been fixed by cycling the safety input through the safe state; which occurs when both channels go LO. Diagnostic Code (13685 decimal) is the indicator that the DCS channels must be cycled.

13. Press flashing green circuit reset button to restart the safety outputs.

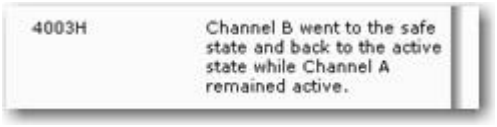
The safety system now allows you to restart the motor. Note that the 1734-IB8S module in slot 2 detected no faults during this procedure. All it knows is that channel 3 went LO when you pressed the 'Estop Wire OFF' button.

Channel Cycled Input Fault

14. Press the EStop Wire OFF button (note it is a maintained button).

15. Press the EStop Wire OFF button again within 3 seconds to generate a **Channel Cycled fault.**

    The Channel cycle fault code 4003h indicates precisely that channel B cycled while channel A was steady. Recall the wire off button affects channel B of the Emergency Stop button.



16. Press the Flashing red EStop DCS icon on the HMI:

17. Press the Fault button on the bottom of the HMI screen:

    The DCS instruction faceplate for the Emergency Stop button provides the exact description of the 4003h code as found in the user's manual. Note that the 1734-IB8S module in slot 2 detected no faults during this procedure. All it knows is that channel 3 went LO and then back HI.

18. Close the instruction faceplate on the HMI using the [X] in the top right corner.

19. Cycle the flashing red selector switch to clear the fault code.

20. Cycle the Emergency Stop button (flashing).

21. Press the flashing green reset push button.

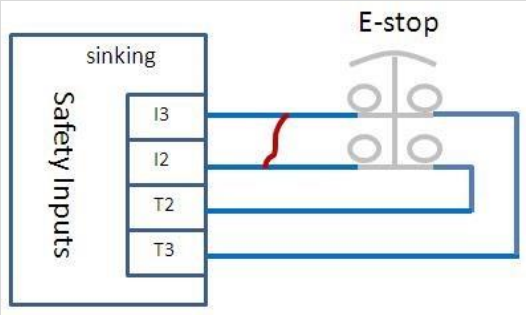
Pulse Test Fault

22. Press the 'ch-ch short' button to create a short between the two Estop channels. (green button to the right of

EStop Wire OFF)

This fault is detected by the next pulse test. The safety I/O module detects this fault because pulse testing is hardware and firmware based within the module itself. The EStop channel LEDs 2 and/or 3 are solid red, indicating a fault.

When the *EStop ch1 to ch2 short* button is pressed, a short is created between the two channels (channel 2 & 3 in slot2).



23. Press the 1734-IB8S slot2 image on the HMI screen to call up the 1734-IB8S faceplate

The faceplate indicates that channels 2 and 3 are faulted

24. Press the flashing yellow alarm bell on the HMI screen.

The HMI indicates 'Estop chB External Test Signal Error', which means the pulse test failed on the Estop channels

25. Select the [?] on the right hand side of the menu bar.

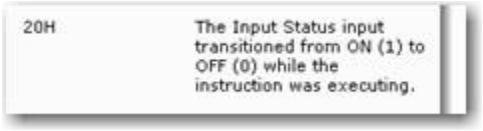
The second probable cause, a channel-to-channel short (short circuit between input signal lines) matches the actual fault.

26. Close the IB8S window on the HMI.

27. Press the Flashing red Estop DCS icon on the HMI

28. Press the Fault button on the bottom of the HMI screen:

The DCS instruction, on the other hand, monitored the input channel status bit(s) of the 1734-IB8S module and declared a fault of 20h because at least one of these status bits unexpectedly went LO during normal execution.



29. Close the instruction faceplate on the HMI using the [X] in the top right corner.

30. Press the ‘ch-ch short’ button again to fix the fault.

31. Cycle the Emergency Stop button (flashing).

To recover from this fault, the safety IO module must sense the input channels in the safe state; both LO. This will require a cycle of the EStop button after the wiring fault has been fixed. The Estop channel LEDs (2 and 3 of the IB8S in slot 2) should be yellow since the fault has been cleared.

32. Cycle red flashing switch to reset the DCS fault.

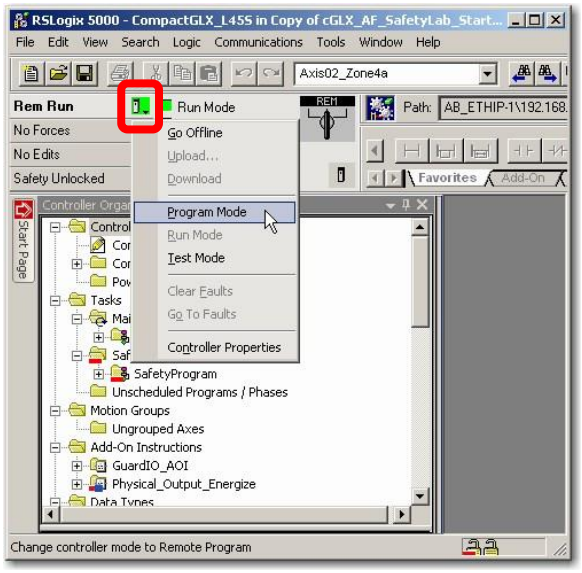
33. Press flashing green button to reset the safety circuits.

34. Close the Controller Tags window using [x] in top right corner of window.

35. Close the safety task ***R01_OB8S_O0_O1*** using the [x] in the top right corner of the window.

Safety Signature

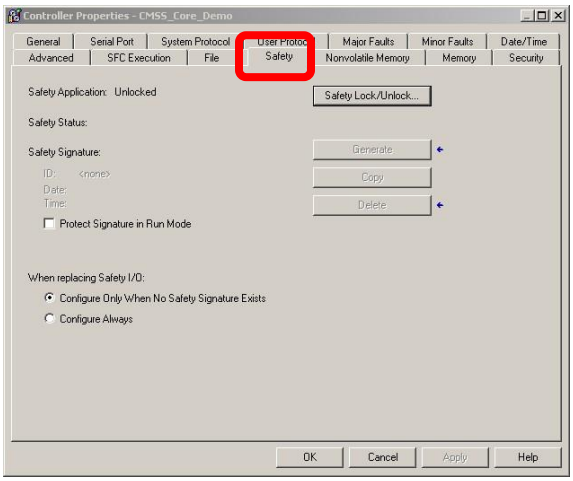
1. While online with RSLogix 5000, place the Compact GuardLogix into Program mode



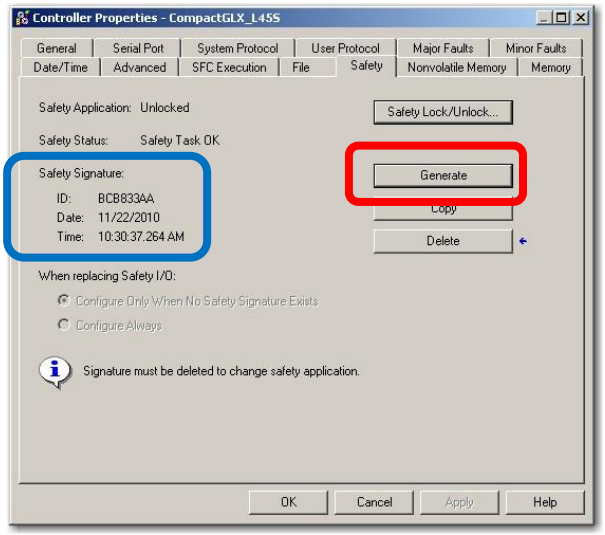
To generate the safety signature, you have to be online and in Program mode.

2. Answer [Yes] to the prompt if performing the mode change using software
3. Call up the controller properties (circled below)

4. Select the *Safety* tab



5. Click on the *Generate* button (circled below).



It takes a few seconds to generate the signature. When complete, the signature will appear in the area circled above in blue. The signature consists of the CRC of safety memory, along with a time date stamp to the millisecond. This guarantees it to be unique.

6. Open up any of the safety routines and notice that the code is grayed out.

To edit the safety task once the signature has been applied, you must delete the safety signature; make the edits; and apply a new signature that has ZERO chance of being the same as the original. So as an OEM, you can generate a safety signature, store the signature in a safe place, and years later if there is a safety incident, you can determine if the safety task has been changed.

7. Close the safety routine

8. Open up any of the standard routines and notice code can still be edited. The safety signature only affects the safety memory.

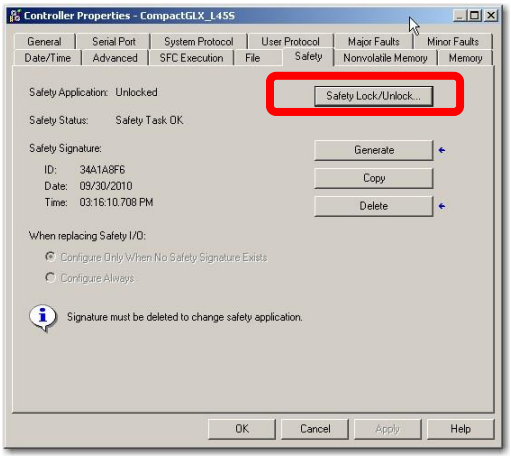
9. Close the standard routine

One last critical point regarding the safety signature is that to operate as a SIL3 controller, the compact GuardLogix must have a safety signature. This is because the memory protection units that are used to prohibit writing to safety memory and the memory check between the primary and partner only operate with a signature in place.

Safety Lock

Once you are running with a safety signature, you need to avoid someone inadvertently downloading a new project to the controller with a different safety task. The safety lock provides this protection.

1. Click the *Safety Lock/Unlock* button (circled below)

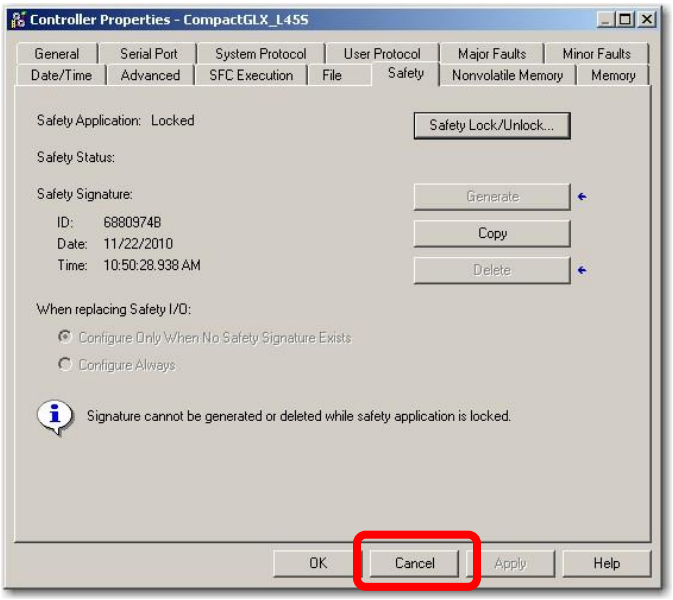


2. Press Lock (circled below)

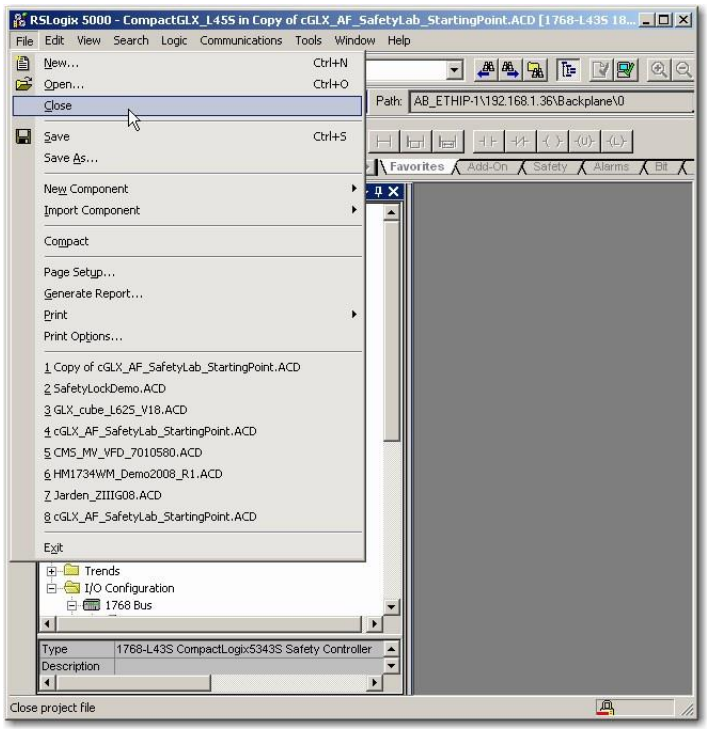
The following will appear in the controller window

When locked, only projects with an identical safety signature can be downloaded to the controller. This enables changes to the standard tasks, while protecting the safety task.

3. Press [Cancel] to close the controller properties window

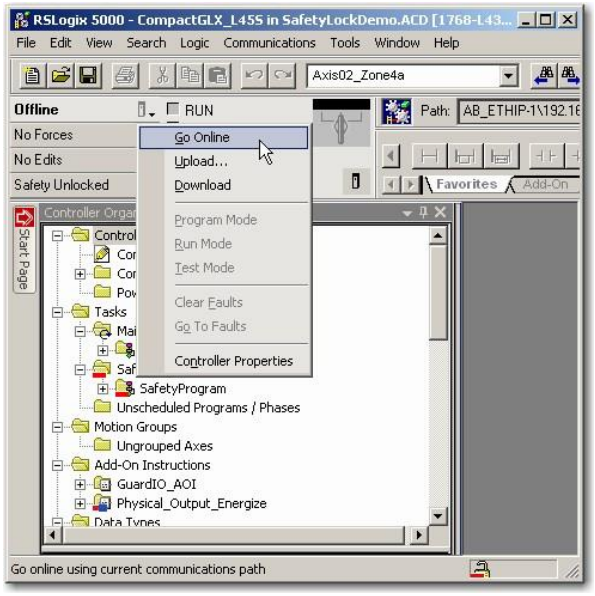


4. Close the ACD file and save the changes when prompted by selecting [Yes]

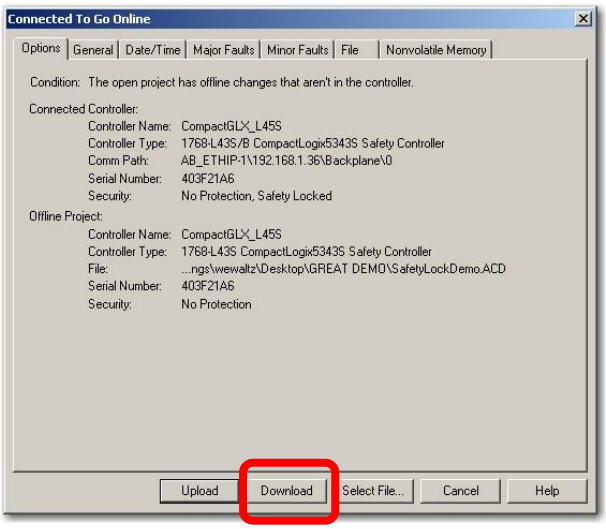


5. Call up the ACD file called **GuardLogix_DCA_SafetyLockDemo.ACD** (located in Lab files folder on desktop)

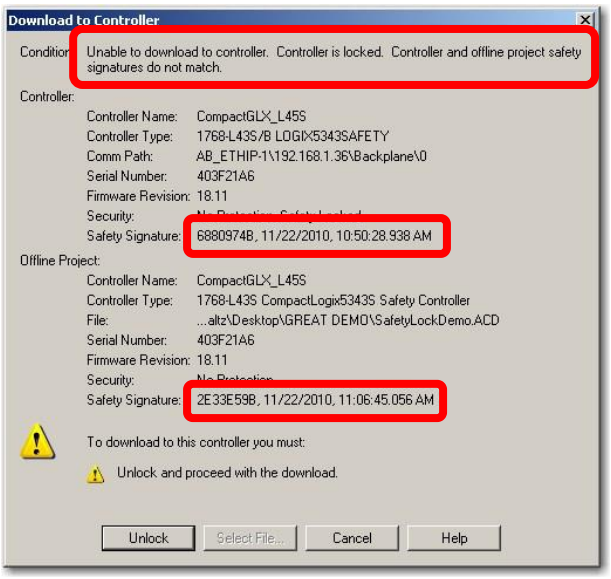
6. Attempt to go online



7. When you see the following window; select Download



The following prompt appears



If you try to download a project with a different safety signature, you will be prompted to unlock the controller. Unlock can be password protected to keep unauthorized users from succeeding. A second purpose of the Lock is to prohibit the deletion of the safety signature. Now the safety program and memory is truly protected from inadvertent changes.

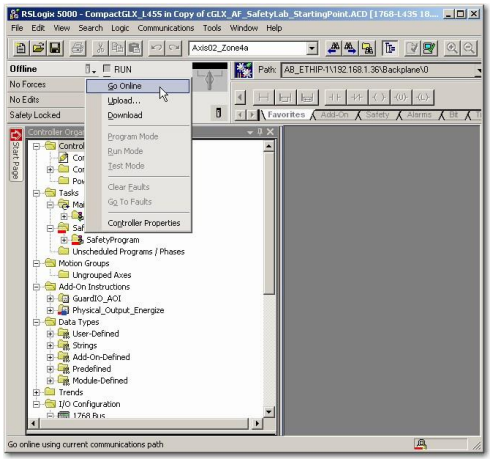
8. Press [Cancel] to close this window

9. Press [Cancel] again to close the online connection window

10. Close the '**GuardLogix_DCA_SafetyLockDemo** project

11. Call up your saved **GuardLogix_StartingPoint.acd** file

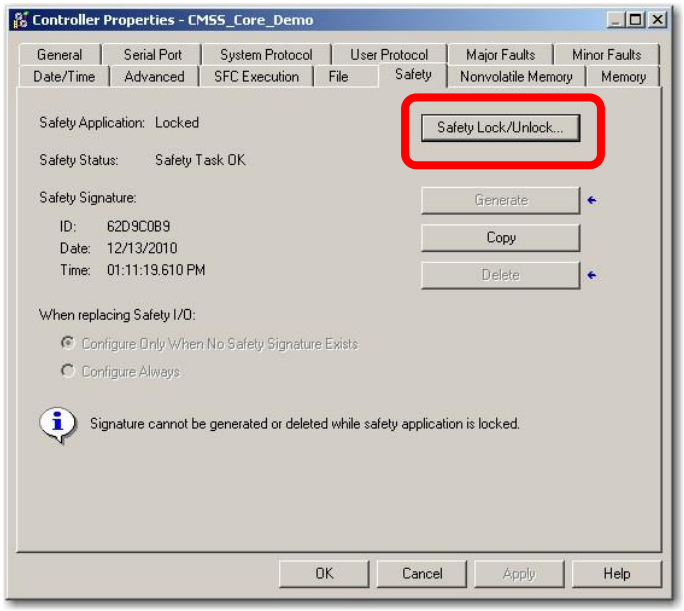
12. Go online



13. Call up the controller properties window

14. Select Safety tab

15. Select Safety Lock/Unlock



16. Select Unlock

17. Select Delete to delete the Safety Signature

18. Answer [Yes] at the prompt

19. Press [Cancel] to close the module properties window

20. Go to Run Mode and answer [Yes] to the prompt

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846